M. Lewenstein[1], B. Kraus[2], P. Horodecki[3], and J. I. Cirac[2]

[1] *Institute for Theoretical Physics, University of Hannover, Hannover, Germany*

[2] *Institute for Theoretical Physics, University of Innsbruck, A–6020 Innsbruck, Austria*

[3] *Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80–952 Gdańsk, Poland*

(May 30, 2000)

We provide a canonical form of mixed states in bipartite quantum systems in terms of a convex combination of a separable state and a, so–called, *edge* state. We construct entanglement witnesses for all edge states. We present a canonical form of nondecomposable entanglement witnesses and the corresponding positive maps. We provide constructive methods for their optimization in a finite number of steps. We present a characterization of separable states using a special class of entanglement witnesses. Finally, we present a nontrivial necessary condition for entanglement witnesses and positive maps to be extremal.

03.67.-a, 03.65.Bz, 03.65.Ca, 03.67.Hk

One of the most fundamental open problems of quantum mechanics is the characterization and classification of mixed entangled states of multipartite systems, i.e., states that exhibit quantum correlations [1]. This problem is of enormous importance for applications in quantum information processing [2–5]. A density operator $\rho \geq 0$ acting on a finite Hilbert space $H = H_A \otimes H_B$ describing the state of two quantum systems A and B is called entangled [6] (or not separable) if it *cannot* be written as a convex combination of product states, i.e., as

$$\rho = \sum_k p_k |e_k, f_k\rangle\langle e_k, f_k|, \tag{1}$$

where $p_k \geq 0$, and $|e_k, f_k\rangle \equiv |e_k\rangle_A \otimes |f_k\rangle_B$ are product vectors. Conversely, ρ is separable (or not entangled) if it can be written in the form (1).

For low dimensional systems (in $H = \mathbb{C}^2 \otimes \mathbb{C}^2$ and $H = \mathbb{C}^2 \otimes \mathbb{C}^3$), there exists an operationally simple necessary and sufficient condition for separability, the so–called Peres–Horodecki criterion [7,8]. It indicates that a state ρ is separable iff its partial transpose is positive, where partial transpose means the transpose with respect to one of the subsystems [9]. However, in higher dimensions this is only a necessary condition; that is, there exist entangled states whose partial transpose is positive (PPTES) [10–12]. Thus, the separability problem reduces to finding whether a density operator with positive partial transpose (PPT) is separable or not [1].

There exists a complete characterization of separable states based on entanglement witnesses (EW) and positive maps (PM) [8]. Briefly speaking: a state ρ is entangled iff there exists a hermitian operator W (an EW) such that $\mathrm{Tr}(W\sigma) \geq 0$ for all separable σ, but $\mathrm{Tr}(W\rho) < 0$. The latter condition offers the possibility of experimental detection of entanglement via the measurement of W – an observable which "witnesses" the quantum correlations in ρ [13]. Starting from EW's one can define PM's [14] that also detect entanglement. An example of a PM is transposition, T [15,16], whose tensor extension $I \otimes T$ detects all non PPT states. Unfortunately, the characterization of EW's and PM's is not known, and therefore the most challenging open questions are: How to construct EW's in general, and what is the minimal set of them which allows to detect all entangled states. First steps toward answering these questions have been accomplished in Ref. [13].

In this Letter we provide a canonical form of mixed states in bipartite quantum systems in terms of a convex combination of a separable state and a so–called *edge* state, which violates extremely the range separability criterion [17]. We construct EW's for all edge states and present a canonical form for nondecomposable EW (nd–EW) and the corresponding PM. We present constructive methods to optimize nd–EW's in a finite number of steps. We provide a characterization of separable states using a special class of EW's that are not necessarily related to edge states, but to certain subspaces of H. Finally, we present a nontrivial necessary condition for nd–EW's and PM's to be extremal. The methods that we use to prove our result are based on the technique of "subtracting projectors on product vectors" [18,19]. Most of the technical proofs have been included in Ref. [20].

In this paper we will denote by $K(\rho)$, $R(\rho)$, and $r(\rho)$ the kernel, range, and rank of ρ, respectively. Let us start by defining the edge states. An "edge" state, δ, is a PPTES such that for all product vectors $|e, f\rangle$ and $\epsilon > 0$, $\delta - \epsilon|e, f\rangle\langle e, f|$ is not positive or does not have a PPT. Obviously, the "edge" states lie on the boundary between PPTES and not PPT states. In order to characterize them we use the following criterion [10,19]:

Criterion: A PPT state δ is an "edge" state iff there exists no $|e, f\rangle \in R(\delta)$ s.t. $|e, f^*\rangle \in R(\delta^{T_B})$.

Note that the edge states violate the range criterion of separability in an extreme manner [10,19]. They are of special importance since they are responsible for the entanglement contained in PPTES's. In order to see that we generalize the method of the best separable approximation (BSA) [18] to the case of PPT states:

Proposition 1: Every PPTES ρ is a convex combination

$$\rho = (1-p)\rho_{sep} + p\delta, \tag{2}$$

of some separable state, ρ_{sep}, and an edge state, δ.

Note that in the decomposition (2) the weight p can be chosen to be minimal [i. e. there exists no decomposition of type (2) with a smaller p].

The decomposition (2) can be obtained using the method of subtracting projectors onto product states $|e,f\rangle \in R(\rho)$ such that $|e,f^*\rangle \in R(\rho^{T_B})$. One can show [18] that $\rho' \propto \rho - \lambda|e,f\rangle\langle e,f|$ is still a PPTES if $\lambda = \min[1/(\langle e,f|\rho^{-1}|e,f\rangle), 1/(\langle e,f^*|(\rho^{T_B})^{-1}|e,f^*\rangle)]$. Moreover, such operation diminishes either the rank of ρ or ρ^{T_B}, or both. The construction of the optimal decomposition is a hard task, but construction of a decomposition with non minimal p can be obtained in a finite number of steps. This provides us with a simple method to construct edge states in arbitrary dimensions, and a separability check [19].

It is natural to ask how to detect PPTES, in the view of the decomposition (2). As mentioned above, one approach is to use EW. There exists a class of EW (called decomposable [20]) which have the form $W = P + Q^{T_B}$, where P and Q are positive operators. Such witnesses can only detect non PPT entangled states [21]. The EW which cannot be written as $W = P + Q^{T_B}$ are called nondecomposable EW. An EW is non–decomposable iff it detects a PPTES [20]. In particular, every nd–EW detects an edge state since one can immediately see from (2) that if $\mathrm{Tr}(W\rho) < 0$ then $\mathrm{Tr}(W\delta) < 0$. Despite their importance, it is not known how to characterize the class of nd–EW's. It is thus an important task to study the EW's of the edge states.

One of the important results of this letter is that for any edge state one can explicitely construct a nd–EW which detects it. To show that, we generalize the method of [13], which is restricted to PPTES constructed out of unextendible product bases [11] which, in particular, do not exist for $2 \times N$ dimensional systems. Let δ be an edge state, C an arbitrary positive operator such that $\mathrm{Tr}(\delta C) > 0$, and P and Q positive operators whose ranges fulfill $R(P) \subseteq K(\delta)$, $R(Q) \subseteq K(\delta^{T_B})$. We define

$$W_\delta \equiv P + Q^{T_B}, \tag{3}$$

and

$$\epsilon \equiv \inf_{|e,f\rangle} \langle e,f|W_\delta|e,f\rangle; \quad c \equiv \sup_{|e,f\rangle} \langle e,f|C|e,f\rangle. \tag{4}$$

Note that the properties of δ ensure that $\epsilon > 0$. We then have

Lemma 1: [Lemma 6 of Ref. [20]] Given an edge state δ, then

$$W_1 = W_\delta - \frac{\epsilon}{c} C \tag{5}$$

is a nd–EW which detects δ.

The simplest choice of P, Q and C consists of taking the projections onto $K(\delta)$, $K(\delta^{T_B})$ and the identity operator, respectively [23]. As we will see below, this choice provides us with a canonical form for nd-EW. In order to show that, let us first introduce some additional notations.

Let $\mathcal{S} \subset \mathcal{P}$ denote the convex set (cone) of separable (resp. PPT) states. Let $\mathcal{P}^\perp \subset \mathcal{S}^\perp$ be the convex sets (dual cones) of nd-EW's (resp. EW's). All those sets are closed.

Definition: An EW (resp. decomposable EW), W is *tangent* to $\mathcal{S}$ (resp. *tangent* to $\mathcal{P}$) if there exists a state $\rho \in \mathcal{S}$ ($\rho \in \mathcal{P}$) such that $\mathrm{Tr}(W\rho) = 0$. Furthermore, we say that W is tangent to $\mathcal{S}$ ($\mathcal{P}$) at $\rho \in \mathcal{S}$ ($\mathcal{P}$) if $\mathrm{Tr}(W\rho) = 0$.

Observation 1: The state ρ is separable iff for all EW's tangent to $\mathcal{S}$, $\mathrm{Tr}(W\rho) \geq 0$.

Proof: (only if) is trivial; (if) Let ρ be an entangled state, and let W be an EW that detects ρ, i.e., $\mathrm{Tr}(W\rho) < 0$. We define $\epsilon \geq 0$ as in (4). If $\epsilon = 0$ then W is tangent to $\mathcal{S}$. If $\epsilon > 0$ then $W' = W - \epsilon\mathbb{1}$ is still an EW which detects ρ and it is tangent to $\mathcal{S}$.

Observation 2: If a decomposable EW, W, is tangent to $\mathcal{P}$ at ρ, then for any decomposition (2) W must also be tangent to $\mathcal{P}$ at the edge state δ.

We can prove now

Proposition 2: If an EW, W, which does not detect any PPTES, is tangent to $\mathcal{P}$ at some edge state δ then it is of the form

$$W = P + Q^{T_B} \tag{6}$$

where $P, Q \geq 0$ such that $R(P) \subseteq K(\delta)$, $R(Q) \subseteq K(\delta^{T_B})$.

Proof: As mentioned before, an EW, W, which does not detect any PPTES must be decomposable; that is, $W = P + Q^{T_B}$. From the PPT property of δ and the positivity of P, Q we have that the ranges $R(\delta)$ and $R(P)$ [resp. $R(\delta^{T_B})$ and $R(Q)$] must be orthogonal.

We are now in the position to prove one of the main results of this paper, regarding our canonical form of nd–EW's:

Proposition 3: Any nd–EW, W, has the form

$$W = P + Q^{T_B} - \epsilon\mathbb{1}, \quad 0 < \epsilon \leq \inf_{|e,f\rangle} \langle e,f|P + Q^{T_B}|e,f\rangle. \tag{7}$$

where P and Q fulfill the conditions of Prop. 2 for some edge state δ.

Proof: Consider $W(\lambda) = W + \lambda\mathbb{1}$. Obviously for some $\lambda > 0$, say λ_0, $W(\lambda_0)$ becomes decomposable. Note that for any $\lambda < \lambda_0$, $W(\lambda)$ is nondecomposable and therefore it detects some PPTES ρ. Using continuity we conclude that $W(\lambda_0)$ is tangent to $\mathcal{P}$. From Obs. 2 there exists an edge state δ to which $W(\lambda_0)$ is tangent. From Prop. 2 we obtain that $W(\lambda_0) = P + Q^{T_B}$, where P and Q satisfy the needed conditions, and consequently $W = P + Q^{T_B} - \epsilon\mathbb{1}$ with $\epsilon = \lambda_0$. Since W is EW, ϵ must not be greater than $\inf_{|e,f\rangle}\langle e,f|P + Q^{T_B}|e,f\rangle$.

Proposition 3': If the assumptions of Prop. 3 hold then W is of the form (7) with $R(P)$, $R(Q)$ orthogonal to some Hilbert subspaces $\mathcal{H}^a$ and $\mathcal{H}^b$, respectively, where: (i) there exists no $|e,f\rangle \in \mathcal{H}^a$ s.t. $|e,f^*\rangle \in \mathcal{H}^b$; (ii) $R[\mathrm{Tr}_B(P_{\mathcal{H}^a})] = R[\mathrm{Tr}_B(P_{\mathcal{H}^b})]$,

$R[\mathrm{Tr}_A(P_{\mathcal{H}^a})] = R[\mathrm{Tr}_A(P_{\mathcal{H}^b})^*]$, where P_X stands for the projector onto the subspace X; (iii) $\dim\mathcal{H}^x > \max[r(\mathrm{Tr}_A(P_{\mathcal{H}^x})), r(\mathrm{Tr}_B(P_{\mathcal{H}^x}))]$, $x = a, b$.
Proof: The point (i) is clear; (ii) and (iii) follow from simple analysis of the ranges of the partial reductions of δ as well as the properties of the range of PPT states [22,19].
Remark 1: The presented formulation permits to release ourselves from dealing with edge states in the canonical decomposition (7). Instead, we may consider only the pairs of "strange" subspaces $H^{a,b}$ of the Hilbert space. Note that the converse of the Proposition 3' is also likely to be true.
Remark 2: It is worth recalling that all EW's are in one to one correspondence to PM's [14]. In particular, any nd-EW leads to a so–called *nondecomposable positive map* (nd-PM), i.e., a map which cannot be written as a convex sum of a completely positive map and some other completely positive map followed by transposition. The characterization of nd-PM's is one of the most challenging open problems in mathematical physics. Prop. 3 (3') thus provides us with a *canonical form for nd–PM.* As we mentioned, a PM Λ (transforming operators acting on $\mathcal{H}_C$ to those acting on $\mathcal{H}_B$) provides a separability test which is stronger than its EW counterpart W_Λ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$. The correspondence between such PM and EW is given by the following relation: if $|\Psi\rangle = \sum_{k=1}^{d_A} |k\rangle_A \otimes |k\rangle_C$ then $W_\Lambda = \mathbb{1}_A \otimes \Lambda(|\Psi\rangle\langle\Psi|)$.

As mentioned above, when studying separability we just have to deal with nd–EW's. In order to reduce the set of nd–EW's and nd–PM's, let us introduce the following definitions. Given two nd–EW's, W_1 and W_2, then we say that W_2 is *nd–finer* than W_1 if all the PPTES detected by W_1 are also detected by W_2. We say that W is a nondecomposable *optimal* (nd–optimal) EW (nd–OEW), if there exists no nd–EW which is nd–finer than W. Thus it is obvious that the nd–EW's we are interested in are the nd–OEW's. Let us call an operator $D = P + Q^T$, with $P, Q \geq 0$ and T denoting the partial transposition with respect to A or B, decomposable. Furthermore let us define the set of product vectors on which the average of W vanishes, i.e., $p_W = \{|e, f\rangle \in H, \text{ s. t. } \langle e, f|W|e, f\rangle = 0\}$. This set plays an important role in the optimization, which can be seen in the following results concerning the characterization of nd–OEW's:
Proposition 4: [Theorem 1b of Ref. [20]] An nd–EW, W, is nd–optimal iff for all decomposable operators D and $\epsilon > 0$ the operator $W' = W - \epsilon D$ is not an EW.
Corollary : If both p_W and p_{W^T} span the whole Hilbert space, $H_A \otimes H_B$, then W is a nd–OEW.
Remark 3: The necessary and sufficient conditions for a nd–EW to be nd–optimal are presented in Ref. [20]. Loosely speaking a nd–EW is nd–optimal iff either both, p_W and p_{W^T} span the whole Hilbert space, or there exist some nonproduct vectors $|\Psi\rangle$ related to p_W (or p_{W^T}) s.t. both, p_W (p_{W^T}) joint with the set of $|\Psi\rangle$ and p_{W^T} (p_W) span the whole $H_A \otimes H_B$. In our numerical studies, however, we have not encountered the latter possibility; it is thus likely that the converse of the Corollary is true.

Our results allow now to design a finite step algorithm to nd–optimize a given EW, W, by subtracting decomposable operators:
(I) Take a decomposable operator, $D = P + Q^T$ such that $Pp_W = 0$ and $Qp_{W^T} = 0$ and check if

$$\lambda_0 \equiv \inf_{|e\rangle \in H_A} \left[D_e^{-1/2} W_e D_e^{-1/2} \right]_{\min} > 0. \tag{8}$$

Here $W_e = \langle e|W|e\rangle$, $D_e = \langle e|D|e\rangle$, where $|e\rangle \in H_A$, whereas $[X]_{\min}$ is the minimal eigenvalue of X.
(II) If λ_0 is positive construct the new, nd–finer EW, $W' = W - \lambda_0 D$.
(III) Iterate the procedure (I)-(II) as long as there is no $D = P + Q^T$ with $Pp_W = 0$ and $Qp_{W^T} = 0$.

After each step the set of p_W, p_{W^T} or both of them increases at least by one element, which is linearly independent of the former ones. So, after a finite number of steps p_W and p_{W^T} will span the whole Hilbert space which ensures that the final nd–EW is nd–optimal. In principle, it may happen that $\lambda_0 = 0$ at some step, before p_W and p_{W^T} span the whole H. Our numerical simulations suggest, however, that among all possible D's one can always find one with $\lambda_0 > 0$.

We have applied the methods of finding and optimizing EW's to a family ρ_b ($b \in [0, 1]$) of PPTES in the 2×4 dimensional system from Ref. [10]. For $b = 0, 1$ those states are separable, whereas for $0 < b < 1$, ρ_b's are edge states which can be checked directly as shown in Ref. [10]. We have applied the following procedure. By virtue of some symmetries of ρ_b, one can perform a local change of basis after which the transformed state $\tilde{\rho}_b$ fulfills $\tilde{\rho}_b^{T_B} = \tilde{\rho}_b$. This step allowed us to construct the nd–EW $W_1 = P + P^{T_B} - \lambda_0 \mathbb{1}$, which detects already the edge state. Following the procedure above we subtracted decomposable operators. In addition we choose them to be invariant under partial transposition with respect to system B. Note that then $W = W^{T_B}$ at any step and therefore we only had to make sure that p_W spanned the whole Hilbert space, which automatically ensured that the final nd–EW was nd–optimal. In Fig. 1 it is shown how many members of the whole family of $\rho_{b'}$'s are detected by the nd–OEW obtained from ρ_b. We plot here also the efficiency of the corresponding nd-PM. Here the improvement of efficency is less spectacular, but still significant.

It must be stressed that both: the EW's and the PM's constructed in 2×4 system are the first examples provided for a quantum system with one qubit subsystem. We have also provided the first examples of the set p_W that spans the whole Hilbert space. This set allows to construct very peculiar separable states of full rank that lie on the boundary of $\mathcal{S}$. Note also that, in general, the parameter λ_0 in the optimization procedure has to be found numerically. In Ref. [20] we have been able to formulate an analytic method that allows to detect the whole family of ρ_b's.

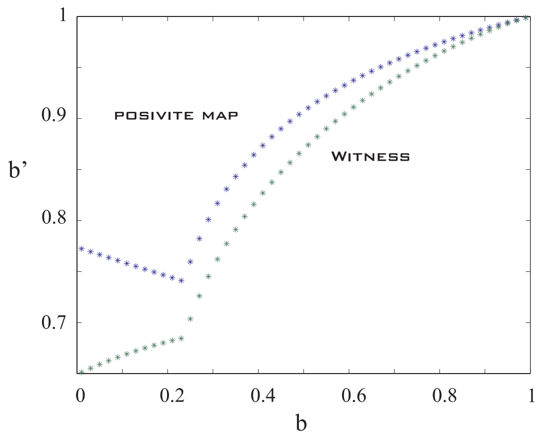

FIG. 1. Values of b' for which if $\tilde{b} \leq b'$, $\tilde{\rho}_{\tilde{b}}$ is detected by the optimal witness and the positive map obtained from $\tilde{\rho}_b$.

As we remember, the key problem is to find the minimal set of EW's detecting PPTES. Obviously, this minimal set will consist of nd-OEW's. A related problem is to find a set of extremal points of $\mathcal{P}^{\perp}$. Note that a nonoptimal nd-EW is a convex sum of an optimal one and a decomposable operator (Prop.4), so it cannot be an extremal point. Note that Prop. 3 (3') combined with the optimality property provides *the necessary form of extremal points* of both EW's, as well as PM's, which has not been known so far. We have thus the following

Proposition 5: The set of extremal points of the set of EW's, $\mathcal{S}^{\perp}$, is contained in the set $\mathcal{A}$ of all optimal EW's of the form (7) plus projectors and transposed projectors.

Proposition 5': The set of extremal points of the cone of nd–EW's, $\mathcal{P}^{\perp}$, is contained in the set $\mathcal{B}$ of all optimal nd-EW's of the form (7).

Remark 4: Moreover, applying the isomorphism [14] to the members of $\mathcal{A}$ ($\mathcal{B}$) we obtain the set $\mathcal{A}'$ ($\mathcal{B}'$) of PM's (nd-PM's) containing the set of all extreme PM's. The above theorems provide thus the first nontrivial necessary condition for EW's and PM's to be extremal. In particular, following Prop. 3' we can obtain a weaker condition by considering optimal EW's of the form (7) without involving the notion of the edge states, but only pairs of "strange" subspaces $\mathcal{H}^a$ and $\mathcal{H}^b$.

This work has been supported by the DFG (SFB 407 and Schwerpunkt "Quanteninformationsverarbeitung"), the DAAD, the ÖFW (SFB "Control and Measurement of Coherent Quantum Systems"), the ESF PESC Programm on Quantum Information, TMR network ERB–FMRX–CT96–0087, the IST Programme EQUIP, and the Institute for Quantum Information GmbH.

[1] M. Horodecki, P. Horodecki and R. Horodecki, in *"Quantum Information - Basic Concepts and Experiments"*, Eds. G. Alber and M. Weiner, in print (Springer, Berlin, 2000).
[2] A. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[4] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] For a review see A. Ekert, R. Jozsa, Rev. Mod. Phys., **68** (1996) 733; A. Steane, Rep. Prog. Phys. **61**, 117 (1998).
[6] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A**223**, 8 (1996).
[9] Given an operator X and an orthonormal basis $\{|k\rangle\}_{k=1}^{N} \in H_B$, one defines the partial transposed of X with respect to B in that basis as follows: $X^{T_B} = \sum_{k,k'=1}^{N} |k'\rangle_B\langle k|X|k'\rangle_B\langle k|$. One can analogously define the partial transposed of X with respect to A in a given basis, X^{T_A}. Partial transposition fulfills the following useful property $\mathrm{tr}(X^{T_B}Y) = \mathrm{tr}(XY^{T_B})$. We say that positive operator has a positive partial transposition (PPT) if $\rho^{T_B} \geq 0$. Note that this property is basis independent.
[10] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[11] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[12] Such states provide examples of the so–called bound entangled states, see M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[13] B. M. Terhal, quant-ph/9810091; see also quant-ph/9911057.
[14] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
[15] E. Störmer, Acta Math. **110**, 233 (1963).
[16] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).
[17] According to this criterium, if ρ is separable then there must exist a set of product vectors $\{|e_k, f_k\rangle\}$ that spans the range $R(\rho)$ s. t. the set of partial complex conjugated product states $\{|e_k, f_k^*\rangle\}$ spans the range of ρ^{T_B}, see [10].
[18] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998); A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A**58**, 826 (1998),
[19] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, quant-ph/9912010; P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac, quant-ph/0002089.
[20] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, quant-ph/0005014.
[21] Optimal decomposable EW can be shown to have the form of the partial transpose of a positive operator whose range does not contain any product vector; see [20].
[22] P. Horodecki, J. A. Smolin, B. M. Terhal, A. V. Thapliyal, quant-ph/9910122.
[23] This choice applied to the entangled states of Ref. [11] reproduces the witnesses constructed in Ref. [13].